

# Non-Binary LDPC Codes with Large Alphabet Size

Koji Tazoe, Kenta Kasai and Kohichi Sakaniwa  
 Department of Communications and Computer Engineering,  
 Tokyo Institution of Technology  
 Email: {tazoe,kenta,sakaniwa}@comm.ce.titech.ac.jp

**Abstract**—We study LDPC codes for the channel with input  $x \in \mathbb{F}_q^m$  and output  $y = x + z \in \mathbb{F}_q^m$ . The aim of this paper is to evaluate decoding performance of  $q^m$ -ary non-binary LDPC codes for large  $m$ . We give density evolution and decoding performance evaluation for regular non-binary LDPC codes and spatially-coupled (SC) codes. We show the regular codes do not achieve the capacity of the channel while SC codes do.

## I. INTRODUCTION

In 1963, Gallager invented low-density parity-check (LDPC) codes [1]. Due to sparsity of the code representation, LDPC codes are efficiently decoded by belief propagation (BP) decoders. By a powerful optimization method *density evolution* [2], developed by Richardson and Urbanke, messages of BP decoding can be statistically evaluated. The optimized LDPC codes can approach very close to Shannon limit [3].

In this paper, we consider non-binary LDPC codes over  $\mathbb{F}_q^m$  defined by sparse parity-check matrices over  $\text{GL}(m, \mathbb{F}_q)$ . Non-binary LDPC codes were invented by Gallager [1]. Davey and MacKay [4] found non-binary LDPC codes can outperform binary ones. Non-binary LDPC codes have captured much attention recently due to their decoding performance [5],[6],[7],[8]. It is observed  $2^m$ -ary non-binary codes exhibit excellent decoding performance around at  $m = 6$  over BMS channels.

Spatially-coupled (SC) codes attract much attention due to their capacity-achieving performance and a memory-efficient sliding-window decoding algorithm. Recently, SC codes are shown to prove achieve capacity of BEC [9], [10] and BMS channels [11].

In this paper, we study coding over the channel with input  $x \in \mathbb{F}_q^m$  and output  $y \in \mathbb{F}_q^m$ . The receiver knows a subspace  $V \subset \mathbb{F}_q^m$  from which  $z = y - x$  is uniformly chosen. Or equivalently, the receiver receives an affine subspace  $y - V := \{y - z \mid z \in V\}$  in which the input  $x$  is compatible. This channel model is used in the decoding process for network coding [12] after estimating noise packet spaces. In [13], the authors proposed a coding scheme with binary SC MacKay-Neal codes with the joint iterative decoding between the channel detector and the code decoder. It was observed that the code exhibits capacity achieving performance for small  $m$ . The channel detector calculates log likelihood ratio (LLR) of the transmitted bits from a channel output and messages from the BP decoder.

The aim of this paper is to evaluate decoding performance of  $q^m$ -ary non-binary LDPC codes for large  $m$ . We give density

evolution and decoding performance evaluation for regular non-binary LDPC codes and SC codes. We show the regular codes do not achieve the capacity of the channel while SC codes do.

## II. CHANNEL MODEL

In this paper, we consider channels with input  $x \in \mathbb{F}_q^m$  and output  $y = x + z \in \mathbb{F}_q^m$ , where  $z \in \mathbb{F}_q^m$  is uniformly distributed in a linear subspace  $V \subset \mathbb{F}_q^m$  of dimension  $\epsilon m$ . It is easy to see that the channel is weakly symmetric [14]. From [14, Theorem 7.2.1], the normalized capacity is given by

$$C = \frac{1}{m} \max_{p(X)} I(X; Y) = (1 - \epsilon).$$

The channel with large  $m$  was used in a decoding process of the network coding scenario [15]. In [15], the data part of each packet is represented as  $x \in \mathbb{F}_q^m$ . Packets are coded by non-binary LDPC codes whose parity-check coefficients are in the general linear group  $\text{GL}(m, \mathbb{F}_q)$ . The noise subspace  $V$  is estimated by padding zero packets and using Gaussian elimination. We denote this channel by  $\text{CD}(m, \epsilon)$ .

## III. CODE DEFINITION

In this section, we briefly review  $(d_l, d_r)$  codes and  $(d_l, d_r, L)$  codes introduced by Kudekar *et al.* [16]. We assume  $\frac{d_r}{d_l} \in \mathbb{Z}$  and  $\frac{d_r}{d_l} \geq 2$ . Both  $(d_l, d_r)$  codes and  $(d_l, d_r, L)$  codes are defined over  $\text{GF}(q)$  and have parity-check matrix over  $\text{GF}(q)$ .

### A. $(d_l, d_r)$ -Codes

Let  $H(d_l, d_r)$  be an  $Md_l \times Md_r$  sparse binary matrix of column weight  $d_l$  and row weight  $d_r$ . The Tanner graph of  $(d_l, d_r, L)$  code is obtained by making  $M$  copies of protographs of  $H(d_l, d_r, L)$  and connecting edges among the same edge types.  $H(d_l, d_r, m)$  is given by replacing 1 with a randomly chosen non-zero elements in  $\text{GL}(m, \mathbb{F}_q)$  and replacing 0 with  $0 \in \text{GL}(m, \mathbb{F}_q)$ , where  $\text{GL}(m, \mathbb{F}_q)$  is the set of all non-singular  $\mathbb{F}_q$ -valued matrix of size  $m \times m$ . The resultant matrix  $H(d_l, d_r, m)$  can be viewed as a  $\text{GL}(m, \mathbb{F}_q)$ -valued matrix of size  $Md_l \times Md_r$ .

### B. $(d_l, d_r, L)$ -Codes

The  $(d_l, d_r, L)$  codes are defined by the following protograph codes [17]. The adjacency matrix of the protograph is referred to as a base matrix. The base matrix of  $(d_l, d_r, L)$  code is given as follow. Let  $H(d_l, d_r, L)$  be an  $(L + d_l - 1) \times \frac{d_r}{d_l} L$

band binary matrix of band size  $d_r \times d_l$  and column weight  $d_l$ , where the band size is height  $\times$  width of the band. We refer to  $L$  as coupling number. For example

$$H(d_l = 4, d_r = 8, L = 9) = \begin{bmatrix} \begin{matrix} 1 & 1 & 1 & 1 & & & & & \\ & 1 & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & 1 & & & \\ & & & 1 & 1 & 1 & 1 & & \\ & & & & 1 & 1 & 1 & 1 & \\ & & & & & 1 & 1 & 1 & 1 \\ & & & & & & 1 & 1 & 1 & 1 \\ & & & & & & & 1 & 1 & 1 & 1 \end{matrix} \end{bmatrix}.$$

The Tanner graph of  $(d_l, d_r, L)$  code is obtained by making  $M$  copies of protographs of  $H(d_l, d_r, L)$  and connecting edges among the same edge types. The parameter  $M$  is referred to as lifting number. The matrix  $H(d_l, d_r, L, M)$  is given by replacing each 1 in  $H(d_l, d_r, L)$  with an  $M \times M$  random permutation and each 0 with an  $M \times M$  zero matrix.  $H(d_l, d_r, L, M, m)$  is given by replacing 1 with a randomly chosen non-zero elements in  $\text{GL}(m, \mathbb{F}_q)$  and replacing 0 with  $0 \in \text{GL}(m, \mathbb{F}_q)$ , where  $\text{GL}(m, \mathbb{F}_q)$  is the set of all non-singular  $\mathbb{F}_q$ -valued matrix of size  $m \times m$ . The resultant matrix  $H(d_l, d_r, L, M, m)$  can be viewed as a  $\text{GL}(m, \mathbb{F}_q)$ -valued matrix of size  $(L + d_l - 1)M \times \frac{d_r}{d_l}LM$ .

#### IV. DECODING ALGORITHM

Let  $\mathcal{H}$  be a  $\text{GL}(m, \mathbb{F}_q)$ -valued matrix given by the construction above. Denote row and column size of  $\mathcal{H}$  by  $\mathcal{M}$  and  $\mathcal{N}$ , respectively. Denote the  $(i, j)$ -th entry of  $\mathcal{H}$  by  $h_{i,j} \in \text{GL}(m, \mathbb{F}_q)$ . Then a codeword  $(x_1, \dots, x_{\mathcal{N}}) \in (\mathbb{F}_q^m)^{\mathcal{N}}$  satisfies parity-check equations

$$\sum_{j \in \partial i} h_{i,j} x_j = 0,$$

for  $i = 1, \dots, \mathcal{M}$  where  $\partial i := \{j \in \{1, \dots, \mathcal{N}\} \mid h_{i,j} \neq 0\}$ .

Sum-product algorithm (SPA) [18] is employed to decode. Without loss of generality, we can assume all-zero codeword was sent to make analysis easier [19]. The SPA tries to marginalize the following function with respect to each  $x_j$  ( $j = 1, \dots, \mathcal{N}$ ).

$$\prod_{j=1}^{\mathcal{N}} \Pr(Y_j = y_j \mid X_j = x_j) \prod_{i=1}^{\mathcal{M}} \mathbb{1}\left[\sum_{j \in \partial i} h_{i,j} x_j = 0\right],$$

where  $\mathbb{1}[\cdot]$  is the indicator function. The SPA message forms a uniform probability vector over a subset of  $\mathbb{F}_q^m$ . The support of each sum-product message forms a linear subspace of  $\mathbb{F}_q^m$  [19].

#### V. DENSITY EVOLUTION ANALYSIS OF $(d_l, d_r)$ -CODES

Denote the message subspace sent along a randomly picked edge connecting symbol nodes to check nodes at the  $t$ -th iteration by  $V^{(t)}$ . Similarly, denote the message subspace sent along a randomly picked edge connecting check nodes to symbol nodes at the  $t$ -th iteration by  $U^{(t)}$ . The initial message subspace  $V^{(0)}$  is given by a uniformly random subspace of

dimension  $m\epsilon$ . Density evolution [19] gives update equations of  $V^{(t)}$  and  $U^{(t)}$  as follows.

$$U^{(t)} = \sum_{i=1}^{d_r-1} V_i^{(t)},$$

$$V^{(t)} = V^{(0)} \cap \bigcap_{i=1}^{d_l-1} U_i^{(t)}.$$

where  $U_i^{(t)}$  and  $V_i^{(t)}$  are iid copies of  $U^{(t)}$  and  $V^{(t)}$ , respectively and  $V_1 + V_2 := \{v_1 + v_2 \mid v_1 \in V_1, v_2 \in V_2\}$ . If  $V^{(t)}$  becomes  $\{0\}$ , decoding is successfully completed.

It is not easy to track  $V^{(t)}$ . Instead, we track the dimension of  $V^{(t)}$ . We define  $\xi^{(t)}$  in order to predict the  $\dim V^{(t)}$ .

*Definition 1:* Define

$$\xi^{(t+1)} = (\xi^{(t)})^{\boxplus(d_r-1)} \quad (1)$$

$$\xi^{(t)} = \epsilon \boxminus (\xi^{(t)})^{\boxplus(d_l-1)}, \quad (2)$$

$$\xi^{(0)} = \epsilon$$

where for  $\xi_1, \xi_2 \in [0, 1]$

$$\xi_1 \boxminus \xi_2 := \max(\xi_1 + \xi_2 - 1, 0),$$

$$\xi_1 \boxplus \xi_2 := \min(\xi_1 + \xi_2, 1).$$

Next Lemma shows  $\frac{1}{m} \dim V^{(t)}$  converges to  $\xi^{(t)}$  in probability.

*Lemma 1:* For any  $\delta > 0$  and  $\epsilon > 0$ , there exists  $m'$  such that for  $m > m'$

$$\Pr\{|\dim V^{(t)} - \xi^{(t)}m| < \delta m\} > 1 - \epsilon.$$

*Proof:* Let  $V_1$  be a uniformly random subspace of dimension  $d_1$  in  $\mathbb{F}_q^m$ , and  $V_2$  a uniformly random subspace of dimension  $d_2$ . Then from [12, Proposition 4.4], it holds that for any  $k \geq 0$  and  $m \geq 0$ ,

$$\Pr\{d_1 \boxminus d_2 \leq \dim(V_1 \cap V_2) < d_1 \boxminus d_2 + k\} \geq 1 - q^{-k - \max(0, m - d_1 - d_2)},$$

$$\Pr\{d_1 \boxplus d_2 - k \leq \dim(V_1 + V_2) < d_1 \boxplus d_2\} \geq 1 - q^{-k - \max(0, m - d_1 - d_2)},$$

where, with abuse of notation, we define  $\boxminus$  and  $\boxplus$  for  $d_1, d_2 \in \mathbb{N}$  as follows

$$d_1 \boxminus d_2 := \max(d_1 + d_2 - m, 0),$$

$$d_1 \boxplus d_2 := \min(d_1 + d_2, m).$$

For  $\xi_1 := d_1/m$  and  $\xi_2 := d_2/m$  it follows that

$$\Pr\left\{\left|\frac{\dim(V_1 \cap V_2)}{m} - \xi_1 \boxminus \xi_2\right| < \frac{k}{m}\right\} \geq \Pr\{d_1 \boxminus d_2 \leq \dim(V_1 \cap V_2) < d_1 \boxminus d_2 + k\} \geq 1 - q^{-k - m \max(0, 1 - \xi_1 - \xi_2)}.$$

From this, for sufficiently large  $m$  such that  $\frac{k}{m} < \delta$  and  $q^{-k - m \max(0, 1 - \xi_1 - \xi_2)} < \epsilon$ , it holds that

$$\Pr\left\{\left|\frac{\dim(V_1 \cap V_2)}{m} - \xi_1 \boxminus \xi_2\right| < \delta\right\} \geq 1 - \epsilon.$$

Similarly, we have

$$\Pr\left\{\left|\frac{\dim((V_1 \cap V_2) \cap V_3)}{m} - \frac{\dim(V_1 \cap V_2)}{m} \boxminus \xi_3\right| < \delta\right\} \geq 1 - \epsilon.$$

The union bound of the two probabilities gives

$$\Pr\left\{\left|\frac{\dim(V_1 \cap V_2)}{m} - \xi_1 \boxminus \xi_2\right| < \delta \text{ and } \left|\frac{\dim((V_1 \cap V_2) \cap V_3)}{m} - \frac{\dim(V_1 \cap V_2)}{m} \boxminus \xi_3\right| < \delta\right\} \geq 1 - 2\epsilon$$

Using the triangle inequality and the fact that  $\boxminus$  is a continuous function, we have

$$\Pr\left\{\left|\frac{\dim((V_1 \cap V_2) \cap V_3)}{m} - (\xi_1 \boxminus \xi_2) \boxminus \xi_3\right| < 2\delta\right\} \geq 1 - 2\epsilon.$$

The same argument is valid for any combinations of  $\boxminus$  and  $\boxplus$  of  $V_i^{(0)}$  ( $i = 0, 1, \dots$ ).  $V^{(t)}$  is an instance of the combinations. Hence the thesis holds.

$$\Pr\{|\dim V^{(t)} - \xi^{(t)}m| < \delta m\} > 1 - \epsilon.$$

*Discussion 1:* From Lemma 1, it follows that even a single parity-check code is enough to achieve the capacity when  $m$  is infinite. However the aim of this paper is not to design codes for  $\text{CD}(m, \epsilon)$ , but evaluate the performance of non-binary codes for large  $m$ .

*Lemma 2:*

$$\sup\{\epsilon \in [0, 1] \mid \lim_{t \rightarrow \infty} \xi^{(t)} = 0\} = \frac{1}{d_r - 1}.$$

*Proof:* It is easy to see that

$$\xi^{\boxplus(d_r-1)} = \min((d_r - 1)\xi, 1), \\ \epsilon \boxminus \xi^{\boxminus(d_l-1)} = \max((d_l - 1)\xi + \epsilon - (d_l - 1), 0).$$

First, we claim that  $\xi^{(t)} \geq \frac{1}{d_r-1}$  for  $t \geq 1$  if  $\epsilon \geq \frac{1}{d_r-1}$ . We use induction. Under the assumption that  $\xi^{(t)} \geq \frac{1}{d_r-1}$ , we can see that

$$\zeta^{(t+1)} = \min((d_r - 1)\xi^{(t)}, 1) = 1 \\ \xi^{(t+1)} = \max((d_l - 1)\zeta^{(t+1)} + \epsilon - (d_l - 1), 0) = \epsilon.$$

Hence, we obtain that for all  $t \geq 0$ ,

$$\xi^{(t)} = \xi^{(0)} \geq \frac{1}{d_r - 1}.$$

Next, we claim that  $\lim_{t \rightarrow \infty} \xi^{(t)} = 0$  if  $0 \leq \epsilon < \frac{1}{d_r-1}$ . It follows that  $0 \leq \zeta^{(t)} < 1$ , (1) and (2) can be rewritten respectively by

$$\xi^{(t+1)} = \max((d_l - 1)(d_r - 1)\xi^{(t)} + \epsilon - (d_l - 1), 0).$$

This can be solved as

$$\xi^{(t)} = \max\left(\frac{(d_l - 1)\{(d_l - 1)(d_r - 1)\}^t}{(d_l - 1)(d_r - 1) - 1}((d_r - 1)\epsilon - 1) + \frac{\epsilon - (d_l - 1)}{1 - (d_l - 1)(d_r - 1)}, 0\right)$$

From this, it can be seen that if  $\epsilon < \frac{1}{d_r-1}$ ,  $\xi^{(t)}$  is monotonically decreasing down to 0.  $\square$

We define the threshold which shows how good the  $(d_l, d_r)$  code is. For  $\epsilon < \epsilon(d_l, d_r)$ ,  $(d_l, d_r)$  codes achieve vanishing decoding error probability.

*Definition 2:* We define the *threshold* of  $(d_l, d_r)$  codes as follows.

$$\epsilon(d_l, d_r) = \sup\{\epsilon \in [0, 1] \mid \lim_{t \rightarrow \infty} \lim_{m \rightarrow \infty} \dim V^{(t)} = 0\}.$$

We say that the  $(d_l, d_r)$  codes achieve capacity of  $\text{CD}(m, \epsilon)$  when  $\epsilon(d_l, d_r) = \frac{d_l}{d_r}$ .

From Lemma 1, Lemma 2 we have the following theorem.

*Theorem 1:* For  $d_l \geq 2$ ,  $\epsilon(d_l, d_r) = \frac{1}{d_r-1}$ .

## VI. DENSITY EVOLUTION ANALYSIS OF $(d_l, d_r, L)$ -CODES

Denote the message subspace sent along a randomly picked edge connecting symbol nodes to check nodes at the  $t$ -th iteration from section  $i$  to section  $j$  by  $V_{i,j}^{(t)}$ . Similarly, denote the message subspace sent along a randomly picked edge connecting check nodes to symbol nodes at the  $t$ -th iteration from section  $i$  to section  $j$  by  $U_{i,j}^{(t)}$ .

The initial message subspace  $V_i^{(0)}$  is given by a uniformly random subspace of dimension  $m\epsilon$  for  $i \in \{0, \dots, L-1\}$  and  $V_i^{(0)} = \{0\}$  for  $i \notin \{0, \dots, L-1\}$ . Density evolution gives update equations of  $V^{(t)}$  and  $U^{(t)}$  as follows.

$$V_{i,i}^{(0)} = V_{i,i+1}^{(0)} = \dots = V_{i,i+d_l-1}^{(0)} = V_i^{(0)}, \\ U_{i,j}^{(t+1)} = \sum_{k=0, k \neq j}^{d_l-1} V_{i-k,k}^{(t)}, \\ V_{i,j}^{(t)} = V_i^{(0)} \cap \left(\bigcap_{k=0, k \neq j}^{d_l-1} U_{i+k,k}^{(t)}\right), \\ V_i^{(t)} = V_i^{(0)} \cap \left(\bigcap_{k=0}^{d_l-1} U_{i+k,k}^{(t)}\right). \quad (3)$$

*Definition 3:* For  $i \notin \{0, \dots, L-1\}$ , we set define

$$\xi_i^{(0)} = \xi_{i,j}^{(0)} = 0$$

For  $i \in \{0, \dots, L-1\}$ , define

$$\xi_i^{(0)} = \xi_{i,j}^{(0)} = \epsilon, \\ \zeta_{i,j}^{(t+1)} = \boxplus_{k=0, k \neq j}^{d_l-1} \xi_{i-k,k}^{(t)}, \\ \xi_{i,j}^{(t)} = \epsilon \boxminus \left(\boxplus_{k=0, k \neq j}^{d_l-1} \zeta_{i+k,k}^{(t)}\right), \\ \xi_i^{(t)} = \epsilon \boxminus \left(\boxplus_{k=0}^{d_l-1} \zeta_{i+k,k}^{(t)}\right).$$

*Lemma 3:* For any  $\delta > 0$  and  $\epsilon > 0$ , there exists  $m'$  such that for  $m > m'$

$$\Pr\{|\dim V_{i,j}^{(t)} - \xi_{i,j}^{(t)} m| < \delta m\} > 1 - \epsilon,$$

$$\Pr\{|\dim V_i^{(t)} - \xi_i^{(t)} m| < \delta m\} > 1 - \epsilon.$$

*Proof:* The proof is similar to that of Lemma 1 and hence omitted.  $\square$

*Lemma 4:*

$$\sup\left\{\epsilon \in [0, 1] \mid \lim_{t \rightarrow \infty} \xi_i^{(t)} = 0, i = 0, \dots, L-1\right\} = \frac{d_l}{d_r}.$$

*Proof:* It sufficient to show that if  $\epsilon = \frac{d_l}{d_r}$ ,  $\xi_i = 0$ . This is due to the fact that  $\frac{d_l}{d_r}$  is the Shannon threshold. First let us check messages from check nodes at section 0 to variable nodes at section 0.

$$\zeta_{0,0}^{(1)} = \overbrace{\epsilon \boxplus \dots \boxplus \epsilon}^{d_r-1} = \frac{d_l}{d_r} \left( \frac{d_r}{d_l} - 1 \right) = 1 - \frac{d_l}{d_r}.$$

We employ peeling decoder [19, p. 30] instead of SPA at section 0. The threshold should be the same [19].

$$\begin{aligned} \xi_0^{(1)} &= \zeta_{0,0}^{(1)} + \zeta_{0,1}^{(1)} + \dots + \zeta_{0,d_l-1}^{(1)} + \epsilon - d_l \\ &\leq \zeta_{0,0}^{(1)} + 1 + \dots + 1 + \epsilon - d_l \\ &= \zeta_{0,0}^{(1)} + \epsilon - 1 = 0. \end{aligned}$$

This implies all symbols at section 0 can be successfully decoded. This reduces  $(d_l, d_r, L)$ -code to  $(d_l, d_r, L-1)$ -code. Repeat the decoding step  $L$  times then all symbols will be decoded.  $\square$

*Definition 4:* We define BP threshold of  $(d_l, d_r, L)$  codes as follows.

$$\epsilon(d_l, d_r, L) = \sup\{\epsilon \in [0, 1] \mid \lim_{t \rightarrow \infty} \lim_{m \rightarrow \infty} \dim V_i^{(t)} = 0\},$$

where  $V_i^{(t)}$  is defined in (3).

From Lemma 3, Lemma 4 and the fact that the  $(d_l, d_r, L)$  codes have rate  $1 - \frac{d_l}{d_r} - \frac{d_l-1}{L}$ , we have the following theorem.

*Theorem 2:* In the limit of large  $m$ , the  $(d_l, d_r, L)$  codes have threshold  $1 - \frac{d_l}{d_r}$ . In the limit of large coupling number  $L$ , the  $(d_l, d_r, L)$  codes achieve the capacity of CD( $m, \epsilon$ ).

$$\lim_{L \rightarrow \infty} \epsilon(d_l, d_r, L) = \frac{d_l}{d_r},$$

$$\lim_{L \rightarrow \infty} \lim_{m \rightarrow \infty} R(d_l, d_r, L) = 1 - \frac{d_l}{d_r}$$

## VII. CONCLUSION

We investigated decoding performance of  $q^m$ -ary non-binary LDPC codes for large  $m$  over CD( $m, \epsilon$ ). We gave density evolution and decoding performance evaluation for regular non-binary LDPC codes and SC codes. We show the regular codes do not achieve the capacity of the channel while SC codes do.

## VIII. CONCLUSION

### REFERENCES

- [1] R. G. Gallager, *Low Density Parity Check Codes*. in Research Monograph series, MIT Press, Cambridge, 1963.
- [2] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.
- [3] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.
- [4] M. Davey and D. MacKay, "Low-density parity check codes over GF( $q$ )," *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165–167, June 1998.
- [5] K. Kasai, T. Tsujimoto, R. Matsumoto, and K. Sakaniwa, "Information reconciliation for QKD with rate-compatible non-binary LDPC codes," in *Proc. Int. Symp. on Inf. Theory and its Applications (ISITA2010)*, Oct. 2010.
- [6] K. Kasai, D. Declercq, C. Poulliat, and K. Sakaniwa, "Multiplicatively repeated non-binary LDPC codes," *IEEE Trans. Inf. Theory*, Sept. 2011, to appear.
- [7] K. Kasai, D. Declercq, and K. Sakaniwa, "Fountain coding via multiplicatively repeated non-binary ldpc codes," *IEEE Trans. Commun.*, vol. 60, no. 8, pp. 2077–2083, 2012.
- [8] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum error correction beyond the bounded distance decoding limit," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1223–1230, 2012.
- [9] S. Kudekar and H. Pfister, "The effect of spatial coupling on compressive sensing," in *Proc. 48th Annual Allerton Conf. on Commun., Control and Computing*, Sept. 2010, pp. 347–353.
- [10] N. Obata, Y.-Y. Jian, K. Kasai, and H. D. Pfister, "Spatially-coupled multi-edge type LDPC codes with bounded degrees that achieve capacity on the BEC under BP decoding," in *Proc. 2013 IEEE Int. Symp. Inf. Theory (ISIT)*, July 2013, pp. 2433–2437.
- [11] S. Kudekar, T. Richardson, and R. Urbanke, "Spatially Coupled Ensembles Universally Achieve Capacity under Belief Propagation," *ArXiv e-prints*, Jan. 2012.
- [12] A. Montanari and R. Urbanke, "Iterative coding for network coding," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1563–1572, 2013.
- [13] K. Kasai, T. Nozaki, and K. Sakaniwa, "Spatially-coupled binary Mackay-Neal codes for channels with non-binary inputs and affine subspace outputs," in *Proc. 2012 IEEE Int. Symp. Inf. Theory (ISIT)*, 2012, pp. 463–467.
- [14] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley Interscience, 2006.
- [15] A. Montanari and R. L. Urbanke, "Coding for network coding," *ArXiv e-prints*, vol. abs/0711.3935, 2007.
- [16] S. Kudekar, T. Richardson, and R. Urbanke, "Threshold saturation via spatial coupling: Why convolutional LDPC ensembles perform so well over the BEC," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 803–834, Feb. 2011.
- [17] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protographs," *IPN Progress Report*, pp. 42–154, Aug. 2003.
- [18] F. Kschischang, B. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.
- [19] V. Rathi, "Non-binary LDPC codes and EXIT like functions," Ph.D. dissertation, Lausanne, 2008. [Online]. Available: <http://library.epfl.ch/theses/?nr=4111>